


# Le temps des Tempest



# Qui sommes-nous ?



- DevSecOps @Icodia
- @n0xyne sur Discord
- <https://n0x.cc>

-  Hardware hacker
- Over caffeinated hyena
- @CyberWolf\_2077



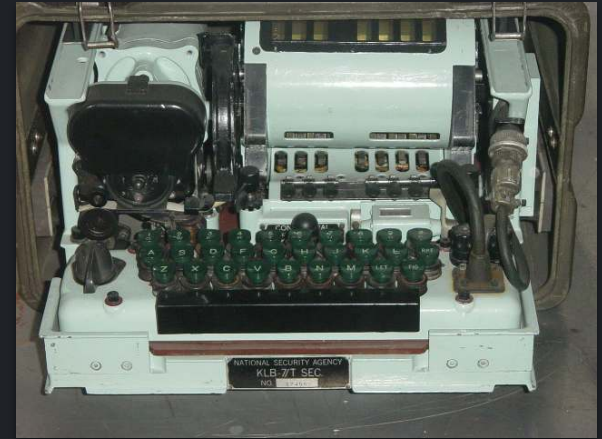
# Qu'est-ce que les risques TEMPEST ?

Telecommunications Electronics Materials Protected from Emanating Spurious Transmissions

- Émission électromagnétique
- Analyses acoustiques
  - Ex: Capture des sons fait par un appareil de chiffrement mécanique, pouvant mener à une récupération du texte clair
- Analyses sismiques (vibrations mécaniques)
  - Ex: Capture des frappes de clavier tactile sur téléphone via l'accéléromètre

Références:

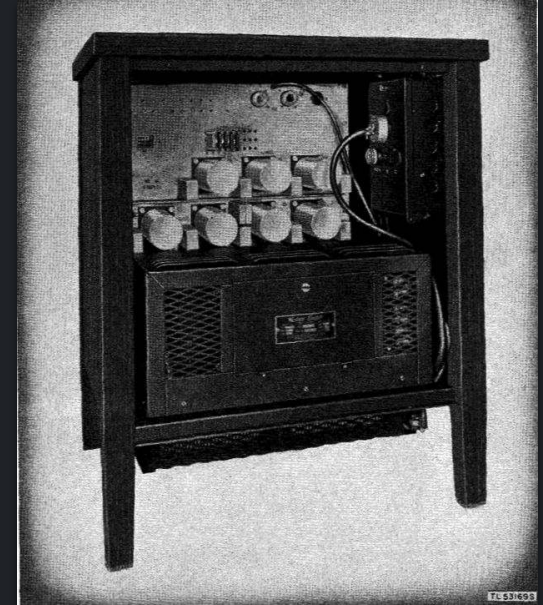
<https://www.nsa.gov/portals/75/documents/news-features/declassified-documents/cryptologic-spectrum/tempest.pdf>



Une machine de chiffrement électromécanique TSEC/KL-7 très utilisée aux USA

# Un peu d'histoire

- Découvert accidentellement en 1942 par Bell lors de la seconde guerre mondiale via une machine de chiffrement (XOR) Bell 131-B2 à plusieurs dizaines de mètres
- Signalé mais non cru par le gouvernement américain
- Démontré publiquement par Bell en récupérant un texte brut via une capture d'un centre cryptographique militaire à 24 mètres de distance



Références:

<https://www.nsa.gov/portals/75/documents/news-features/declassified-documents/cryptologic-spectrum/tempest.pdf>

[https://www.governmentattic.org/2docs/Hist\\_US\\_COMSEC\\_Boak\\_NSA\\_1973.pdf](https://www.governmentattic.org/2docs/Hist_US_COMSEC_Boak_NSA_1973.pdf)



# Un peu d'histoire

- Début des normes NAG-1 en 1959
- Découverte suite à des tests que les téléscripteurs utilisés sont lisibles jusqu'à 1 kilomètre lors d'essai sur le terrain.  
(augmentation des périmètres et interdiction d'utilisation hors USA)



Un téléscripteur Friden Flexowriter très utilisé aux USA dans les années 1950-60

Références:

<https://www.nsa.gov/portals/75/documents/news-features/declassified-documents/cryptologic-spectrum/tempest.pdf>



# Un peu d'histoire

- Découverte en 1962 d'antennes espionnes dans un centre cryptographique américain au Japon
- Découverte en 1964 de 40+ microphones dans l'ambassade américaine à Moscou
- Augmentation drastique des moyens mis dans les contre mesures





# Un peu d'histoire

- Publication et démonstration, en 1985 par Wim van Eck, de capture d'écran cathodique à une distance de 100 mètres pour seulement 15\$
- Révélations de Snowden en 2013 sur la surveillance de masse et quelques informations de TEMPEST activement exploités
- Déclassification de documents sur TEMPEST
- Amélioration des outils open-source et des protections



Références:

<https://www.nsa.gov/portals/75/documents/news-features/declassified-documents/cryptologic-spectrum/tempest.pdf>



# Matériel sensible aux ROEM

Tout matériel électronique, mais plus particulièrement :

- Claviers, souris, imprimantes, fax, ...
- Écrans (VGA, DVI, HDMI, DisplayPort)
- Casques, haut-parleurs, microphones
- Microcontrôleurs, processeurs, etc.
- Accéléromètre, gyroscopes, capteur de vibration (capture téléphone mobile)
- Électro-aimants

Références:

[https://eudl.eu/pdf/10.1007/978-3-319-92213-3\\_6](https://eudl.eu/pdf/10.1007/978-3-319-92213-3_6)

<https://www.cise.ufl.edu/~traynor/papers/marq-ccs11.pdf>

<https://www.repository.cam.ac.uk/items/a778309a-db3d-4ee9-ba40-b49a45a8b922>

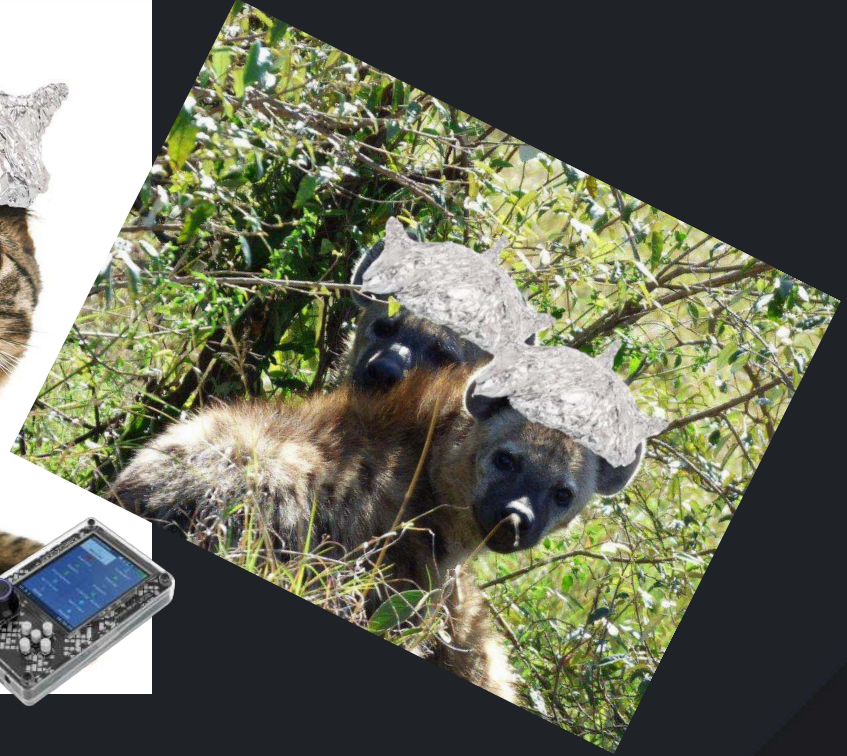
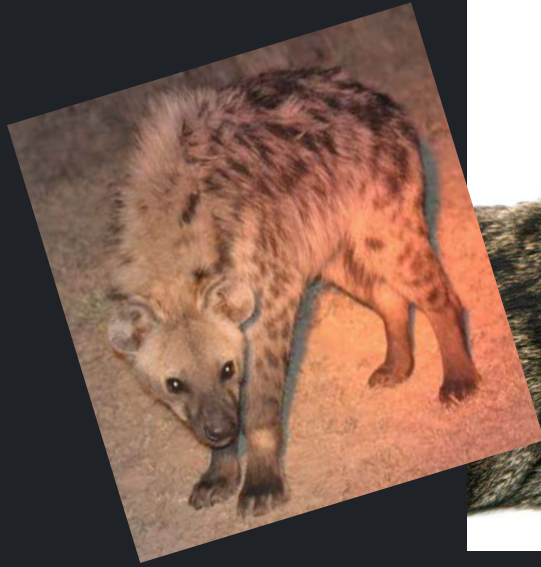
@Bière Sécu Rennes – 13 mai 2025



**TLP:CLEAR**



# Bonnes raison d'être parano

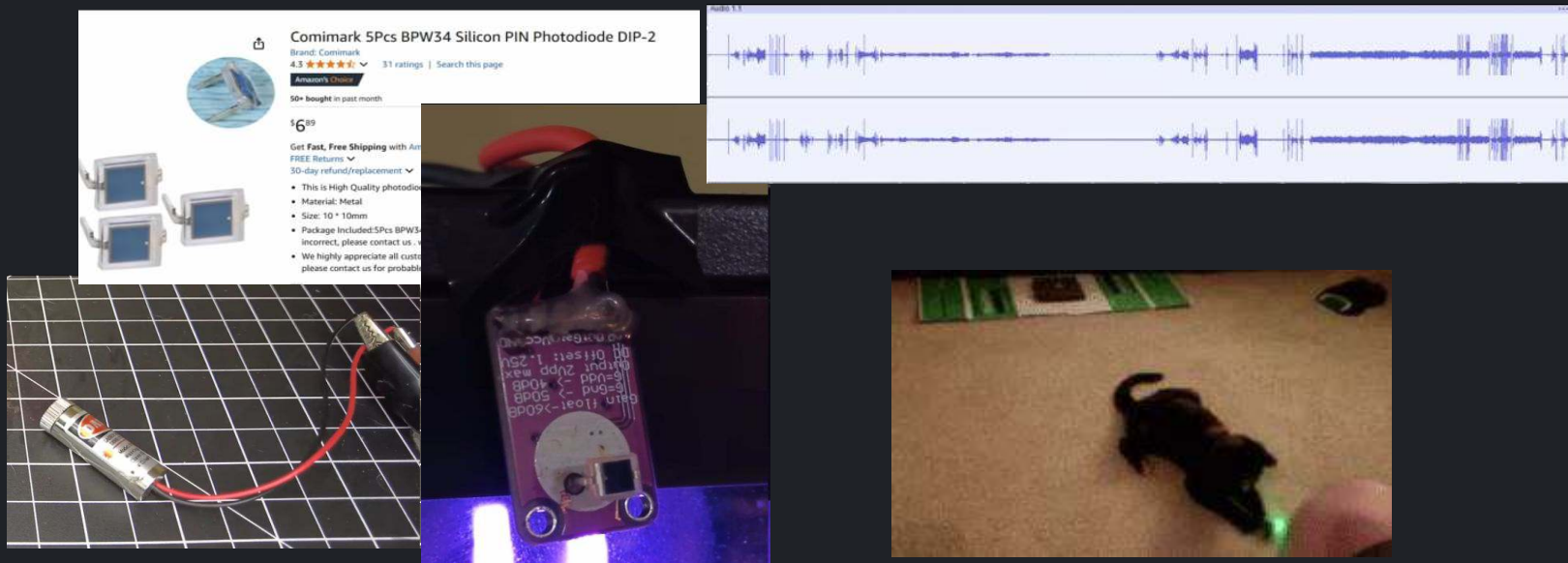


# Réseau ECHELON & Five Eyes

- Coopération de renseignement entre l'Australie, le Canada, la Nouvelle-Zélande, le Royaume-Uni et les États-Unis.
- Découvert en 1988.
- Utilisation d'installations proche de points de départ et d'arrivée de câbles sous-marins de télécommunications intercontinentales.



# Bonnes raisons d'être parano – laser mic



Références:

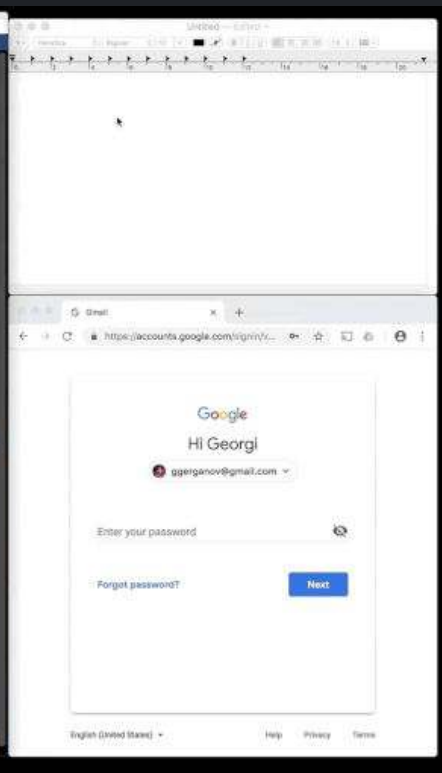
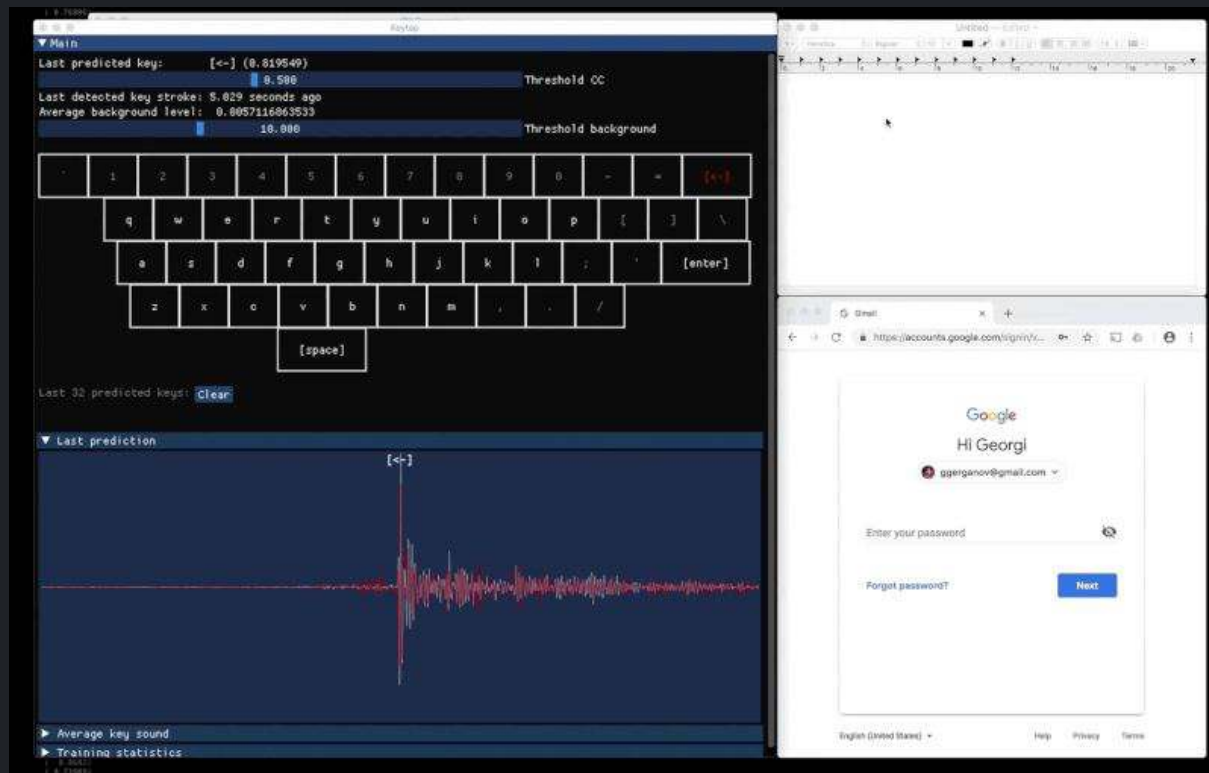
<https://youtu.be/EiVi8AjG4OY>



# Bonnes raisons d'être parano – keystroke capture



Références:  
<https://keytap.ggerganov.com/>



TLP:CLEAR



# Bonnes raisons d'être parano – capture d'écran

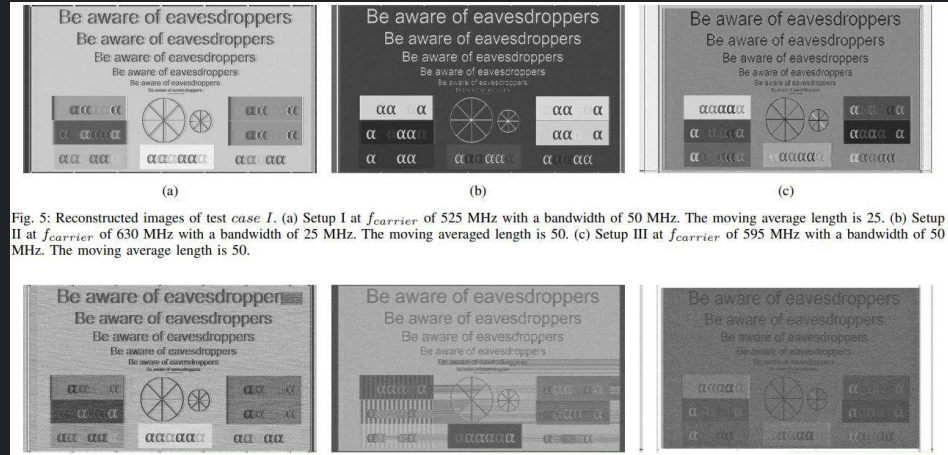


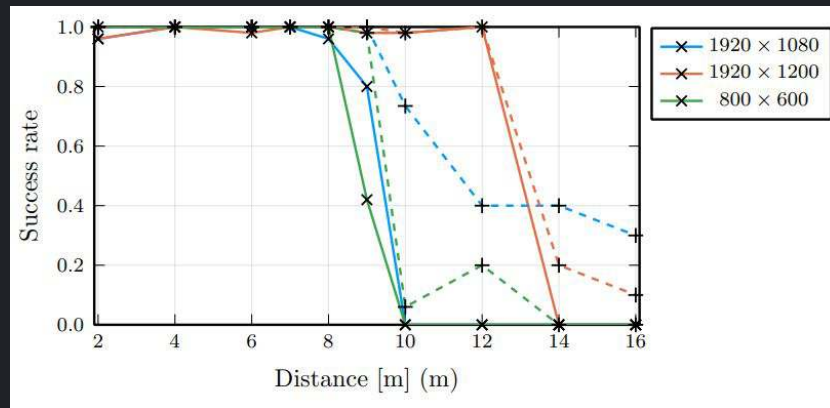
Fig. 5: Reconstructed images of test case I. (a) Setup I at  $f_{\text{carrier}}$  of 525 MHz with a bandwidth of 50 MHz. The moving average length is 25. (b) Setup II at  $f_{\text{carrier}}$  of 630 MHz with a bandwidth of 25 MHz. The moving averaged length is 50. (c) Setup III at  $f_{\text{carrier}}$  of 595 MHz with a bandwidth of 50 MHz. The moving average length is 50.

Références:

[https://www.researchgate.net/publication/344820281\\_Eavesdropping\\_a\\_Ultra-High-Definition\\_Video\\_Display\\_from\\_an\\_80\\_Meter\\_Distance\\_Under\\_Realistic\\_Circumstances](https://www.researchgate.net/publication/344820281_Eavesdropping_a_Ultra-High-Definition_Video_Display_from_an_80_Meter_Distance_Under_Realistic_Circumstances)



# Bonnes raisons d'être parano – capture d'écran



Références:

<https://www.repository.cam.ac.uk/items/a778309a-db3d-4ee9-ba40-b49a45a8b922>



# Le début de l'enfer – Capture DP

74

## 4.2. SCRAMBLER CODE PHASE TRACKING

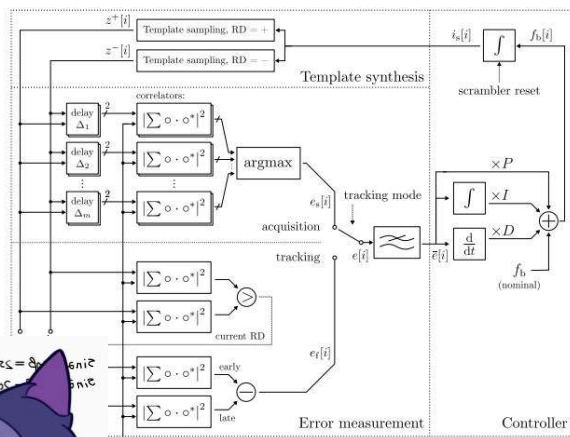
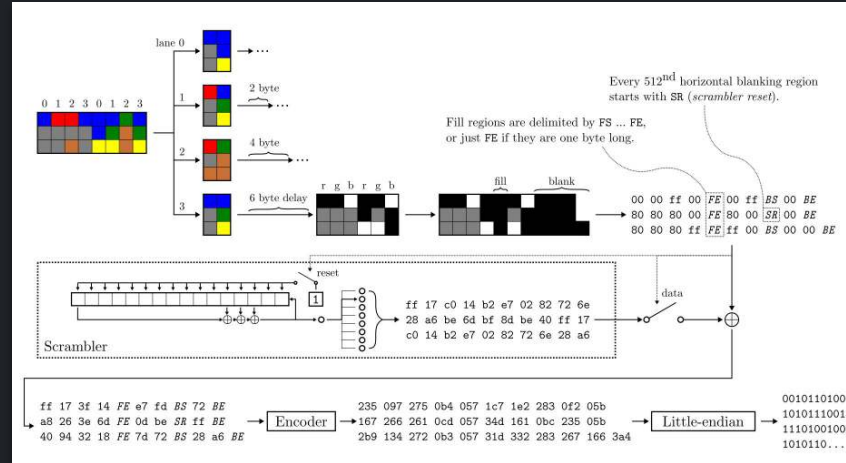


Figure 4.2: Overview of the scrambler tracking algorithm.



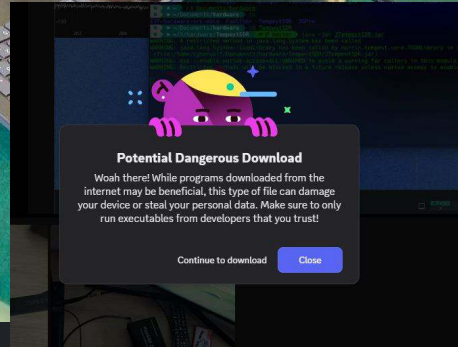
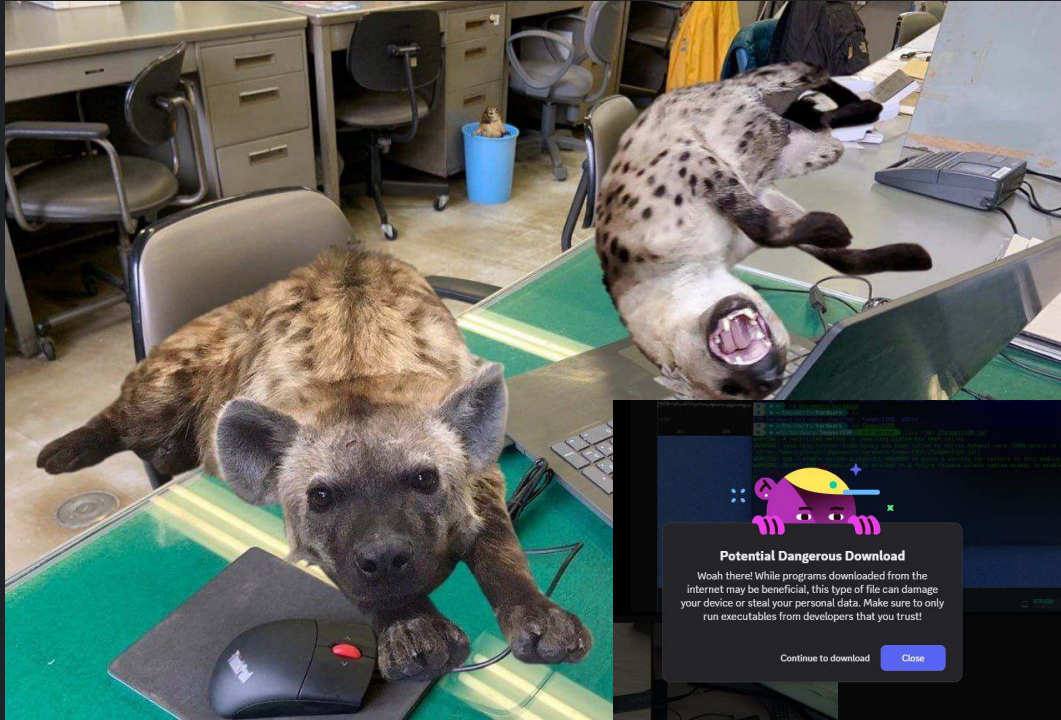


# Les outils utiles

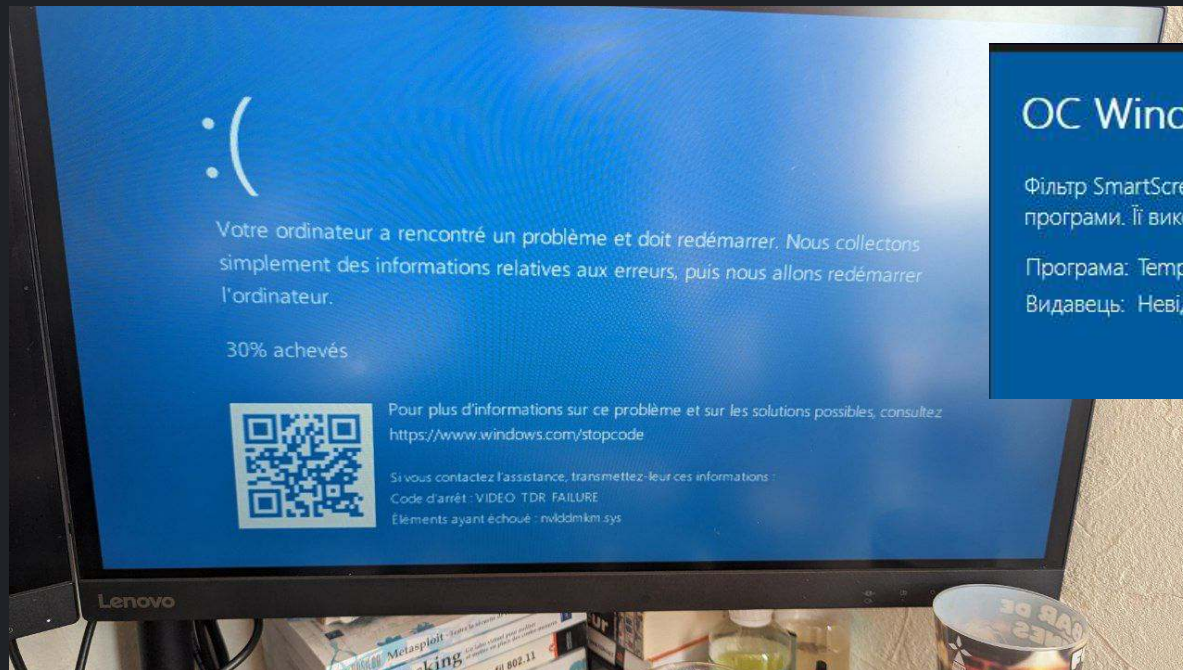
- Une SDR
- Des antennes
- TempestSDR
- GNURadio
- SDRSharp / SDRAngel (enfin qui as les plugins pour votre SDR quoi 🤪)
- gr-tempest
- De la chance et du courage



# La suite de l'enfer (please make hyena friendly softwares)



# On m'as dit sur Windows ça marche mieux ( cé fo )



## ОС Windows захистила цей ПК

Фільтр SmartScreen для Microsoft Defender запобіг запуску нерозпізнаної програми. Її виконання може становити небезпеку для ПК.

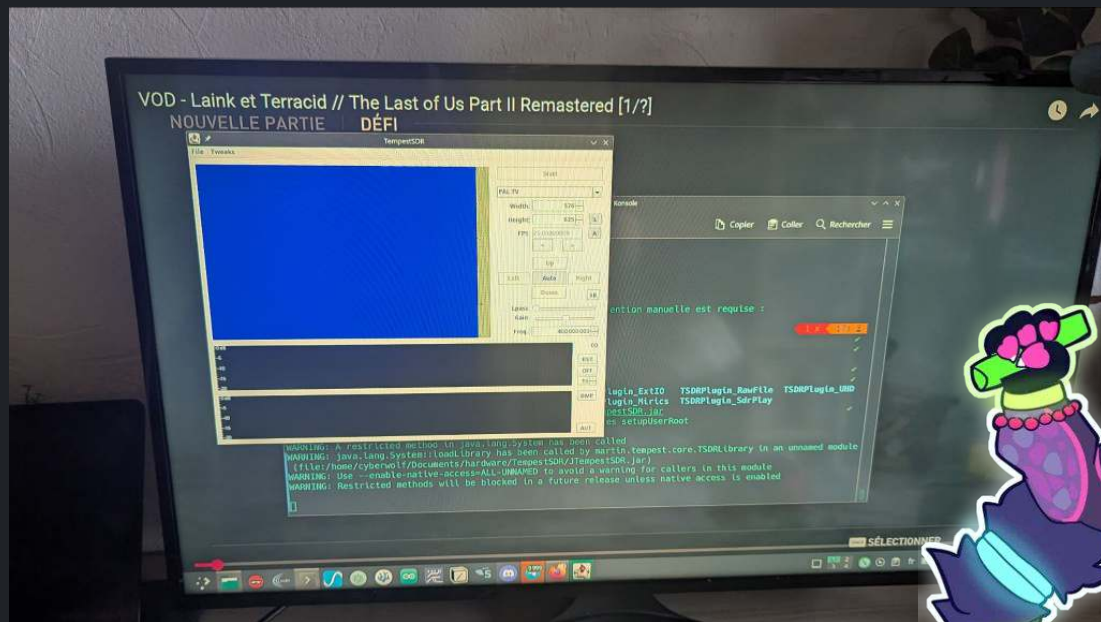
Програма: TempestSDR.exe

Видавець: Невідомий видавець

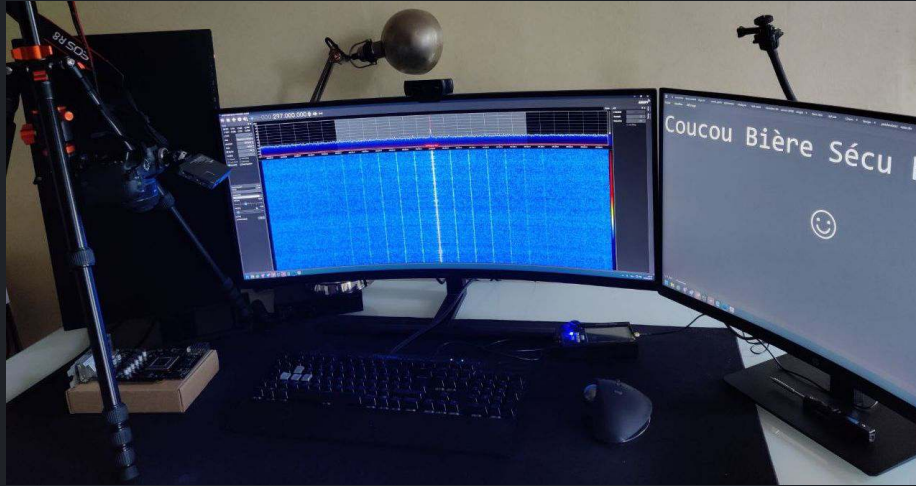




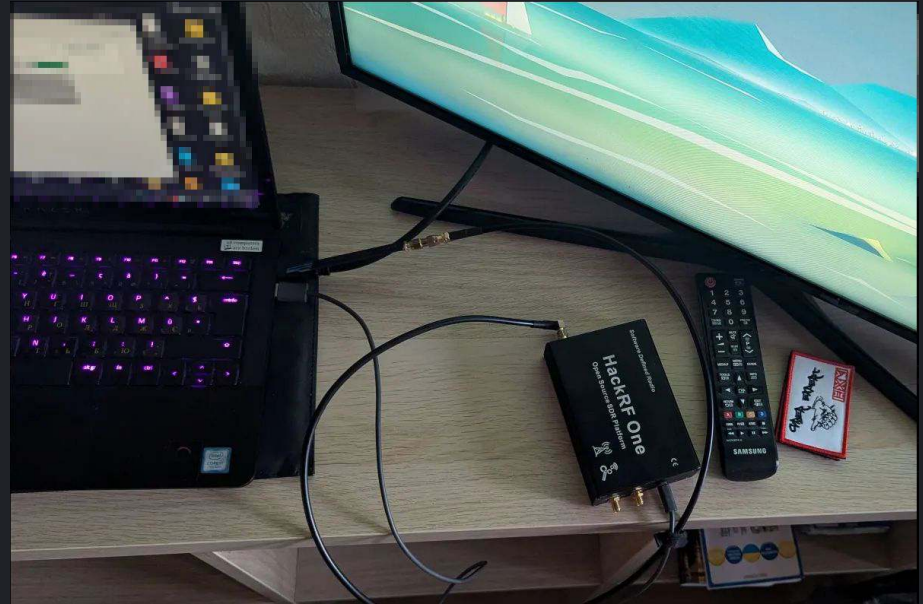
# Quand soudain



# Nos setup



# Nos setups capture



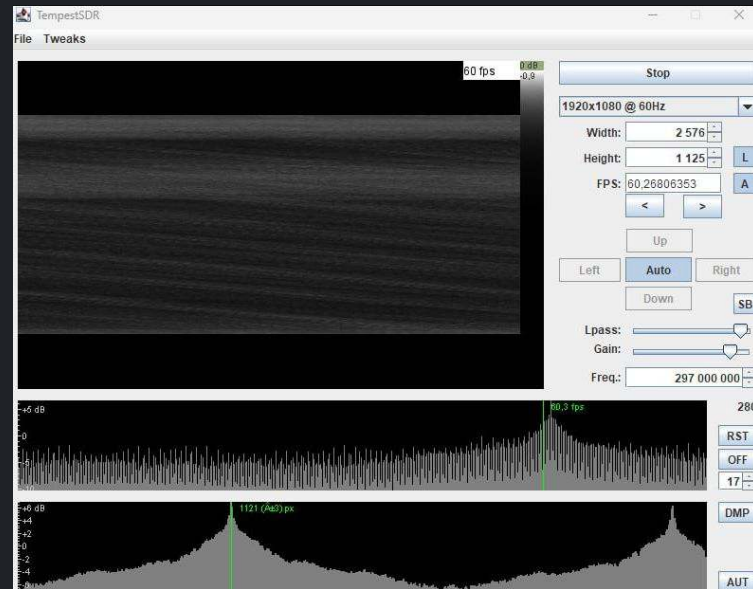


# Le résultat

ça marche vraiment pas mal



ou pas .....





# Le setup idéal (si nos OnlyFans fonctionnaient mieux)

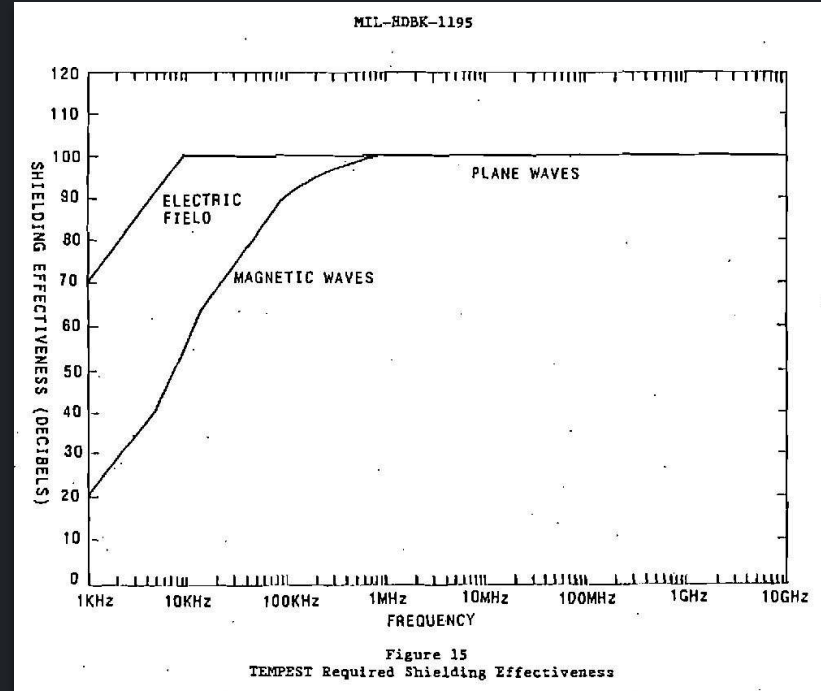


# Protection contre les ROEM

- Blindage (dans une certaine mesure)
- Distanciation (zone de sécurité autour du matériel sensible)
- Bruit (Perturbation des émissions)
- Distanciation entre les câbles et composants transmettant des données sensible de ceux transmettant des données non sensible (Séparation RED/BLACK)

Références:

<https://cryptome.org/tempest-2-95.htm>



Document déclassifié sur le blindage nécessaire en fonction de la fréquence



# Protection contre les ROEM



Chambre anéchoïque



*Les parois sont recouvertes d'absorbants électromagnétiques définis selon la plage de fréquence désirée :*

*Absorbants ferrite SEA-FE, bande de fréquences : 30 MHz – 1 GHz*

*Absorbants mousses pyramidaux SEA-PM, bande de fréquences : 800 MHz – 40 GHz*

# POC – Capture de signaux HDMI

Matériel :

- HackRF One (fonctionne aussi avec une RTL-SDR à 5€)
- Écran 1920x1080@60 connecté en HDMI
- Antenne pouvant capturer entre 100MHz et 400MHz



# Conclusion

Maintenant, on aura peur tous ensemble ! 😏





# Questions

**MY LAST TWO BRAINCELLS  
WATCHING ME STRUGGLE**

